CONTINUATION OF AN APPLICATION FOR A SEARCH WARRANT

I, Marcel Behnen, being duly sworn, state as follows:

INTRODUCTION AND BACKGROUND

1. I make this continuation as part of an application for a search warrant under Rule 41 of the Federal Rules of Criminal Procedure, 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), for information associated with an account that is stored at premises owned, maintained, controlled, or operated by Apple, Inc. ("Apple"), an electronic communications service provided and/or remote computing service, headquartered at One Apple Park Way, Cupertino, California. The information to be searched is Apple ID "christophergreen635@gmail.com" (the "**Subject Account**"), as described in the following paragraphs and in Attachment A. This search warrant will require Apple to disclose to the government copies of information (including the contents of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will then review that information to locate and seize the items described in Section II of Attachment B.

2. I previously submitted a search warrant (1:25-mj-130) for Apple iCloud account christophergreen**365**@gmail.com, which contained a typographical error. The correct iCloud account for the "**Subject Account"** is christophergreen**635**@gmail.com, as listed above, and in Attachment A. Otherwise, this application is identical to the previous application that was submitted to the court and authorized by the U.S. Magistrate Judge Ray Kent on March 6, 2025.

3. I am a Task Force Officer with the United States Drug Enforcement Administration, United States Department of Justice, and have been so since March 2019. I have been a police officer with the Kalamazoo Department of Public Safety (KDPS) for about 16.5 years, the last 8.5 of which I have been assigned as an investigator with the Kalamazoo Valley Enforcement Team (KVET), which is tasked with investigating narcotics trafficking. I am currently assigned to the Grand Rapids District Office in the DEA's Detroit Field Division. During my time as a KVET Investigator, I have participated in investigations of unlawful drug trafficking and, among other things, have conducted or participated in surveillance, the execution of search warrants, debriefings of informants, reviews of taped conversations and drug records, and have participated in investigations that included the interception of wire and electronic communications. Through my training, education, and experience, I have become familiar with the manner in which illegal drugs are transported, stored, and distributed, the methods of payment for such drugs, the laundering of narcotics proceeds, and the dialect, lingo, and coded language used by narcotics traffickers. In connection with my duties, I investigate criminal violations of the Federal and State controlled substance and firearm laws including, but not limited to, conspiracy and attempt to possess with intent to distribute and to distribute controlled substances, in violation of 21 U.S.C. § 846; possession with intent to distribute and distribution of controlled substances, in violation of 21 U.S.C. § 841(a)(1); use of communication facilities to facilitate drug trafficking offenses, in violation of 21 U.S.C. § 843(b); possession of a firearm in furtherance of

drug trafficking, in violation of 18 U.S.C. § 924(c); felon in possession of firearms, in violation of 18 U.S.C. §922(g)(1); conspiracy to commit money laundering, in violation of 18 U.S.C. § 1956(h); and money laundering, in violation of 18 U.S.C. § 1956(a)(1)(A)(i), 18 U.S.C. § 1956(a)(1)(B)(i), and 18 U.S.C.§ 1957.

4. The facts in this application come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This application is intended to show merely that there is sufficient probable cause for the requested warrant, and does not set forth all of my knowledge about this matter.

5. Based on my training and experience, the facts as set forth in this application, and my knowledge of this investigation, there is probable cause to believe that violations of 21 U.S.C. §§ 841(a)(1) and 846 have been committed, are being committed, and will be committed by CHRISTOPHER TIRRELL GREEN, and his associates, known and unknown. I further submit that there is probable cause to believe that the **Subject Account** is being used by GREEN to facilitate his drug trafficking activities and that, finally, there is probable cause to search the information described in Attachment A for evidence of these crimes, as described more fully in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), (c)(1)(A). Specifically, the Court is a "district court of the United

States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

A. Background

6. Christopher Tirrell GREEN is a 49-year-old resident of Kalamazoo, MI. GREEN has the following prior felony convictions:

(a) 1994 – Receiving and Concealing Stolen Property (Kalamazoo, MI)

(b) 1996 – Controlled Substance Delivery/Manufacture less than 50 grams (Kalamazoo, MI)

(c) 2008 – Possession with Intent to Distribute Cocaine Base (Federal – Western District of Michigan)

(d) 2016 – Leaving the Scene of an Accident Resulting in Death/Serious Impairment (Kalamazoo, M)

B. GREEN is a Drug Trafficker

7. In November 2024, investigators with the Kalamazoo Valley Enforcement Team (KVET) were investigating another drug trafficker, KW, for distribution of cocaine and ultimately obtained a State of Michigan search warrant for KW's apartment, person, and vehicle.

8. On November 20, 2024, KVET sought to execute the search warrant. On this day, investigators located and surveilled KW. They watched KW drive to the Ridgeway Circle Apartments, park his/her vehicle, and proceeded to the common entry door of 4612 Ridgeway Circle. KW was then let inside of the building. A few

seconds later, KVET investigators watched KW walk out of the same door to the apartment complex, this time carrying what appeared to be a white 13-gallon trash bag with a blue draw string.

9. KVET investigators approached KW, stopped him/her, and searched his/her person. Investigators located a baggie of 20.81 grams of cocaine HCL and one baggie of 27.81 grams of cocaine base on KW's person. Investigators left the area with KW to continue their investigation into KW and execute the search warrant at his/her apartment.

10. Investigators also searched the white 13-gallon trash bag which KW was carrying when he/she walked out of Ridgeway Circle Apartments. Inside they located four large clear plastic wraps/packages, some of which contained a white powder residue which tested positive for cocaine HCL during a presumptive field test. This packaging was consistent with the wrapping/packaging of kilograms of cocaine. A photo of this plastic wrapping is depicted below:

11. Believing KW had met with his/her source of supply just prior to being stopped by law enforcement, investigators spoke with KW. KW admitted that he/she had just obtained the cocaine and crack cocaine found on his/her person from an

individual at 4612 Ridgeway Circle who asked him/her to throw out the trash as well. KW did not know the name of the person, only knew him as "Burger" or "Cash Burger." KW stated that the drug transaction happened just inside of the front entryway of the apartment complex. KW stated that he/she has been dealing with "Burger" or "Cash Burger" for the last three to four months.

12. KW gave investigators consent to review one of his/her cell phones. They found the phone number KW used to call "Burger" / "Cash Burger", 269-XXX-2083.[1] The call log showed several outgoing calls to this numbers on this day leading up to KW's detainment and arrest. KW also showed investigators his/her CashApp and identified the user "$cashburger113" with the name "Christopher GREEN" as the individual he/she knew as "Burger" / "Cash Burger" and whom he/she received the cocaine and crack cocaine from earlier that same day at the Ridgeway Circle Apartments. Investigators then showed KW a photograph of Christopher Tirrell GREEN. KW positively identified GREEN as "Burger" / "Cash Burger," the source of the cocaine, and the subject that handed him/her the trash bag containing the suspected kilo wrappers.

13. Investigators continued to research GREEN and discovered the following:

a. A gray Jaguar SUV, Michigan registration 22ADL1, was parked outside of 4612 Ridgeway Circle, registered to GREEN (at a

[1] I am aware of the full phone number and can provide the Court that number upon request. I have omitted the full phone number here to protect personally identifiable information.

different address).

b. A credible and reliable law enforcement database (CLEAR) was checked and listed an address of 4612 Ridgeway Circle Apt L for GREEN.

c. A KDPS call for service was located, in September 2024, in which officers responded to an assault on Ridgeway Circle involving GREEN and his wife, but no specific apartment was provided.

14. Still on November 20, 2024, KVET conducted a trash pull from the apartment complex's shared trash dumpster. They located a white 13-gallon trash bag with a blue ties, similar to the one that KW said he/she got from "Burger" / "Cash Burger". Inside of that trash bag investigators found additional clear plastic packaging containing white powder residue which a presumptive field test determined to be cocaine HCL.

15. KVET Investigator Raul Bugarin obtained a State of Michigan search warrant for 4612 Ridgeway Circle, Apt L, signed by a Kalamazoo County magistrate/judge late in the day on November 20, 2024.

16. KVET executed the search warrant the same day it was authorized. When they entered 4612 Ridgeway Circle, Apt L, investigators found GREEN standing inside. GREEN was the only occupant inside of the apartment.

17. During the search of 4612 Ridgeway Circle, Apt L, investigators located the following:

a. In the kitchen/dining room:

- $550 of U.S. currency on the kitchen table.
- On the kitchen counter, a red solo cup sitting on top of a digital scale covered with white powder residue (determined to be cocaine HCL by the Kalamazoo Forensic laboratory).
- Knotted baggie containing a baggie of 22.02 grams of cocaine HCL and 73.34 grams of cocaine by the Kalamazoo Forensic Laboratory.
- Additional drug trafficking equipment, including a Pyrex measuring cup with white residue, a "Bella" blender with white residue inside of it, blue scrappers, lottery tickets, boxes of Ziploc bags (gallon and sandwich sized), and baking soda.

b. In the living room:

- In the couch armrest, American Tactical M1911, .45cal handgun and a loaded magazine for that handgun (the magazine was not in the firearm.)
- $10,706 of U.S. currency in a drawer under the living room table.

c. In the bedroom:

- In a plastic trash bin, a three one-gallon ziploc bag containing a total of 11 knotted sandwich bags of white powder determined to total 1,371.97 grams of cocaine HCL by the Kalamazoo Forensic Laboratory.

Below is an image of the cocaine, U.S. currency, and handgun seized from GREEN's apartment:

18. Additionally, two cell phones were located during the search. A black Moxee cell phone in a black case (Subject Device 1) was located in the kitchen, on the counter next to the dixie cup and digital scale covered in cocaine residue. A blue iPhone 15 Pro in a black OtterBox case (Subject Device 2) was also located in the master bedroom, lying on the bed. Collectively the phones were identified as the "Subject Devices" on a previous federal search warrant and continuation, 1:25-mj-111, authorized on February 28, 2025, by U.S. Magistrate Judge Phillip J. Green.

19. GREEN was the only occupant of the apartment. Although it was two-bedroom apartment, only one of the bedrooms was in use (the other had no bed and very little property), there was only one toothbrush in the only bathroom, documents for GREEN and only men's clothing were located.

20. I called the phone number KW had in his phone which he/she identified as belonging to GREEN, 269-366-2083, and Subject Device 1 rang.

21. An ATF nexus examiner reviewed the American Tactical M1911

handgun, found in GREEN's couch armrest. The nexus expert determined that the firearm was manufactured and/or distributed outside the State of Michigan.

22. GREEN was arrested on State of Michigan charges for controlled substance trafficking and firearms possession and lodged at the Kalamazoo County Jail.

23. On February 25, 2025, GREEN was indicted by a federal Grand Jury in the Western District of Michigan on charges of possession with intent to distribute cocaine, in violation of 21 U.S.C. § 841(a)(1), and Felon in Possession of a Firearm, in violation of 18 U.S.C. § 922(g)(1). (Case 1:25-cr-00023-RJJ)

24. Based on my training an experience I know that drug trafficking is a cash business. In my experience, drug traffickers will possess firearms or keep them nearby to protect themselves, their valuable product, and the proceeds of their drug sales.

C. Identification of the Subject Account

25. On March 4, 2025, I conducted a data extraction of Subject Device 2, pursuant to the federal search warrant referenced above. During the extraction process, I learned Subject Device 2 had reverted to a "Before First Unlock" state, meaning much of the data on the device is encrypted and cannot be unencrypted without knowledge of GREEN's passcode for the device.

26. Through the partial data extraction, I was also able to learn the device showed an owner of "Christopher Green." the account associated with the device was that of the **Subject Account**, christophergreen635@gmail.com, and the device was

last backed up to the iCloud on November 20, 2024. This was the same date of the KVET search warrant resulting in the seizure of cocaine, a firearm, and US Currency from GREEN's apartment.

27. Based on my training, experience, and knowledge of this investigation, I know that it is not uncommon for drug traffickers to utilize multiple cellphones. Specifically, drug traffickers frequently compartmentalize phone numbers for family members or certain members of their drug trafficking network that distribute various quantities and types of narcotics. Furthermore, I know it is common to utilize iCloud backup to transfer contacts, ongoing drug conversations and photographs among these various cellphones.

BACKGROUND REGARDING APPLE[2]

28. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

29. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop

[2] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT2039943; "iCloud," available at http://www.apple.com/icloud; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; "iOS Security," available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and "iCloud: How Can I Use iCloud?," available at https//support.apple.com/kb/PH26502.

applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.

c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple's servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud

Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

d. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

e. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

30. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email

provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

31. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

32. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot

pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

33. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

34. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located

on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

35. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

36. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my

training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

37. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

38. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

39. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

40. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

REQUEST FOR SEALING AND NON-DISCLOSURE

41. I respectfully request that the Court order that all papers in support of this application, including the Continuation and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize the investigation and its effectiveness.

42. I am further advised by the U.S. Attorney's Office that the notice requirement of Fed. R. Crim. P. 41(f)(1)(C) applies to Apple, not to the subscriber or customer, pursuant to 18 U.S.C. § 2703(b)(1)(A). Although the Government is not

required to provide notice to the subscriber or customer, I am aware that Apple has instituted a business policy of notifying customers of the receipt of legal process unless ordered by a court not to do so. The U.S. Attorney's Office has advised me that 18 U.S.C. § 2705(b) provides authority for the Court to command the recipient of a warrant or other order issued under Section 2703 not to notify any other person of the existence of such warrant or order if the Court finds reason to believe that such notice would result in danger to a person's life or safety, flight from prosecution, destruction of evidence, witness intimidation, or other serious jeopardy to an investigation. I request that the Court order Apple not to disclose the existence of this warrant because I believe it would cause GREEN and others who he is conspiring with to destroy evidence and/or flee prosecution. Although Section 2705(b) does not set a time limit for the duration of a non-disclosure order, I submit that a period of 180 days, subject to extension upon a showing of need by the Government, would be reasonable.

AUTHORIZATION REQUEST

43. Based on the foregoing, I request that the Court issue the proposed search warrant.

44. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of

the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

45. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.